

## ABSTRACT

A data security device of a USB storage medium reader-writer includes a USB mass storage level controller and at least one data protection device provided within the USB storage medium reader-writer, in which the USB mass storage level controller controls the USB data communication between a USB host computer and the data protection device. The data protection device includes a writing protection unit, an encrypting unit, and a decrypting unit. The USB host computer may send out a control command to the writing protection unit, the encrypting unit, and the decrypting unit through the USB mass storage level controller, so that when data are written to the data storage medium of the USB storage medium reader-writer, the writing protection unit and the encrypting unit can perform data writing protection and encrypting actions; and when data are read from the data storage medium, the decrypting unit can perform decrypting action. The present utility model is a security device having data writing protection and encryption and data reading decryption functions.

[12] 实用新型专利说明书

[21] ZL 专利号 02202146.9

[45] 授权公告日 2002 年 11 月 27 日

[11] 授权公告号 CN 2522936Y

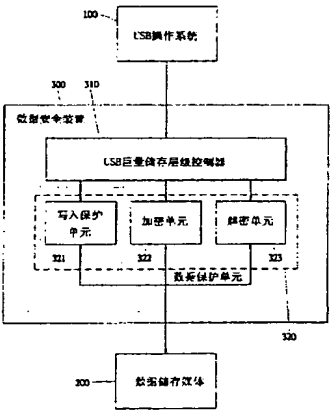
[22] 申请日 2002.01.22 [21] 申请号 02202146.9  
[73] 专利权人 茂杰国际有限公司  
地址 台湾省台北县中和市中山路三段 120 - 11 号 6 楼  
[72] 设计人 刘培中

[74] 专利代理机构 上海专利商标事务所  
代理人 任永武

权利要求书 1 页 说明书 6 页 附图 5 页

[54] 实用新型名称 USB 储存媒体读写器的数据安全装置  
[57] 摘要

一种 USB 储存媒体读写器的数据安全装置,包括一 USB 巨量储存层级控制器及至少一数据保护装置,设于上述 USB 储存媒体读写器内,其中,USB 巨量储存层级控制器负责控制 USB 数据传输于 USB 作业主机及数据保护装置间,该数据保护装置包括一写入保护单元、加密单元及解密单元,让 USB 作业主机可以通过 USB 巨量储存层级控制器,对写入保护单元、加密单元或解密单元下达控制命令,以使放入 USB 储存媒体读写器内的数据储存媒体进行数据写入时,通过写入保护单元及加密单元分别作数据写入保护及加密动作;以及,在数据由数据储存媒体读出时,由解密单元进行解密,本实用新型为一具有数据写入保护、加密及数据读出解密的安全装置。



ISSN 1008-4274

1. 一种 USB 储存媒体读写器的数据安全装置，其特征在于，包括：

— USB 巨量储存层级控制器连结于一 USB 操作系统与数据保护装置之间，并执行 USB 操作系统送来的 USB 协议命令；以及

至少一数据保护装置，连结于 USB 巨量储存层级控制器及数据储存媒体间，包括一写入保护单元、加密单元及解密单元；该写入保护单元及加密单元在数据写入模式下，对数据储存媒体进行数据写入保护及写入加密；在对数据储存媒体进行数据读出模式下，对已加密的数据储存媒体中的数据进行自动解密再送到 USB 操作系统。

2. 如权利要求 1 所述的 USB 储存媒体读写器的数据安全装置，其特征在于，USB 巨量储存层级控制器及数据保护装置纳置于一 USB 储存媒体读写器中。

3. 如权利要求 2 所述的 USB 储存媒体读写器的数据安全装置，其特征在于，该 USB 储存媒体读写器为 USB 卡片阅读机。

4. 如权利要求 1 所述的 USB 储存媒体读写器的数据安全装置，其特征在于，该数据保护装置所连结的数据储存媒体是 CF、MMC、SM 或 SD 存储器组件。

## USB 储存媒体读写器的数据安全装置

### (1) 技术领域

本实用新型有关一种 USB 储存媒体读写器的数据安全装置, 尤指一种用于 USB 储存媒体读写器, 及具有数据写入保读、加密及解密组件的数据安全装置。

### (2) 背景技术

CF (COMPACT FLASH) 存储器、MMC (MEMORY STICK) 存储器、SM (smart media) 存储器及 SD (secure digital 存储器, 广泛使用作为巨量数字数据的储存媒体, 例如: 应用在数字相机中, 用来记录数字相机所拍摄的影像数值数据。然而, 在这些存储器组件的应用过程中, 是通过现有的储存媒体读写器, 如卡片阅读机 (card reader) 来作为数据读、写的媒介, 但并没有为这些数据储存媒体设计数据写入保护的保护措施, 无法避免数据被随意篡改或不慎消除的危险。

另外, 在这些数据储存媒体经过卡片阅读机进行数据读、写的操作过程中, 缺乏数据读、写的安全保密机制, 任何人只要取得他人的数据储存媒体, 均可以轻易地查阅内容资料及进行档案、资料的复制、传递, 对于个人资料保密而言是一隐忧。

如考虑在上述的各项数据储存媒体上设计以数据防止写入保护或安全保密的硬件措施, 则将使得该数据储存媒体的硬件规格被改动, 造成数据储存媒体无法统一, 且要由该数据储存媒体上直接加设以硬件线路的保护装置, 则显得相当困难不易, 并且, 使卡片阅读机的硬件也需一并被改变, 这并不符合产业利用的需求及经济效益。

### (3) 实用新型内容

本实用新型的主要目的是在于提供一种 USB 储存媒体读写器的数据安全装置, 包括一 USB 巨量储存层级控制器 (USB MASS STORAGE CLASS controller) 及至

少一数据保护装置，设于 USB 储存媒体读写器内，以在不改受数据储存媒体硬件结构前提下，达到数据保护的效果。

本实用新型的另一目的是提供一种 USB 储存媒体读写器的数据安全装置，特别是该数据保护装置具有一写入保护单元，可以直接由 USB 作业主机下达写入保护命令而使数据储存媒体防止数据被任意写入。

本实用新型的又一目的是提供一种 USB 储存媒体读写器的数据安全装置，该数据保护装置具有一加密单元，可以直接由 USB 作业主机下达加密命令，而使数据储存媒体于数据写入时加密。

本实用新型的再一目的是在于提供一种 USB 储存媒体读写器的数据安全装置，该数据保护装置具有一解密单元，可以直接由 USB 作业主机下达解密命令，使数据储存媒体内已加密的数据读出时被自动解密。

为实现上述目的，本实用新型的 USB 储存媒体读写器的数据安全装置，包括一 USB 巨量储存层级控制器(US MASS STORAGECLASS controller)及至少一数据保护装置，设于上述 USB 储存媒体读写器内；其中，USB 巨量储存层级控制器负责控制 USB 数据传输于 USB 作业主机及数据保护装置间，该数据保护装置则包括一写入保护单元、加密单元及解密单元，让 USB 作业主机可以通过 USB 巨量储存层级控制器，对写入保护单元、加密单元或解密单元下达控制命令，以使放入 USB 储存媒体读写器内的数据储存媒体进行数据写入时，通过写入保护单元及加密单元分别作数据写入保护及加密动作；以及，在数据由数据储存媒体读出时，由解密单元进行解密。

为进一步说明本实用新型的目的、结构特点和效果，以下将结合附图对本实用新型进行详细的描述。

#### (4)附图说明

图 1 为本实用新型的系统方块图；

图 2 为本实用新型的写入保护单元进行数据写入保护的流程图；

图 3 为本实用新型的加密单元进行数据写入加密的流程图；

图 4 为本实用新型的解密单元进行数据读出解密的流程图；

图 5 为本实用新型的较佳应用例图。

### (5)具体实施方式

首先请参阅图 1 所示, 为本实用新型的系统方块图, 本实用新型的 USB 储存媒体读写器的数据安全装置(以下称数据安全装置), 其中, 在图 1 中的 USB 操作系统 100 是指具有 USB 接口的作业装置或平台, 如个人计算机、笔记型计算机, 而数据储存媒体 200 则是泛指如 CF (COMPACT FLASH) 存储器、MMC (MEMORY STICK) 存储器、SM (SMART MEDIA) 存储器或 SD (SECURITY DIGITAL) 存储器等巨量数据储存媒体。

本实用新型的数据安全装置 300, 是设在一 USB 储存媒体读写器 400 中(如图 5 所示), 其中, 该数据安全装置 300 包括一 USB 巨量储存层级控制器(USB MASS STORAGE CLASS controller) 310 及至少一数据保护装置 320, 该 USB 巨量储存层级控制器 310 是使用 USB MASS STORAGE CLASS 规格中所定义的 BULK. ONLY 或 CBI 协议来对 USB 操作系统 100 与数据保护装置 320 间进行存取或读、写, 使 USB 储存媒体读写器 400 在放入上述的数据储存媒体 200 进行数据读写时(请参考图 5 所示), 可以被 USB 操作系统 100 视为一即插即拔 (PLUG AND PLAY) 的硬盘、CD-ROM 或磁盘驱动器使用。

该数据保护装置 320 连结至上述 USB 巨量储存层级控制器 310 与数据储存媒体 200 间, 该数据保护装置, 还包括有一写入保护单元 321、加密单元 322 及解密单元 323, 其中, 写入保护单元 321 可以在 USB 操作系统 100 对数据储存媒体 200 进行数据写入情况下, 可作数据写入保护设定, 也就是可以通过 USB 操作系统 100 向 USB 巨量储存层级控制器 310 下达数据写入保护设定命令, 而由 USB 巨量储存层级控制器 310 控制写入保护单元 321 的启动或关闭, 而设定数据储存媒体 200 禁止数据写入或允许数据写入; 加密单元 322 则是在 USB 操作系统 100 对 USB 巨量储存层级控制器 310 下达对数据储存媒体 200 进行数据写入情况下, 由加密单元 322 对 USB 巨量储存层级控制器 310 所送来的写入数据进行加密保护, 使数据在写入数据储存媒体 200 时均作保密。

上述的解密单元 323 在于 USB 操作系统 100 对数据储存媒体 200 进行数据读入的情况下, 由 USB 巨量储存层级控制器 310 对解密单元 323 下达解密

命令，使通过 USB 储存媒体读写器 400 所读入的数据储存媒体 200 中的数据，先进行判断是否有加密，如为无加密的数据，则无需解密直接通过 USB 巨量储存层级控制器 310 送到 USB 操作系统 100 中；倘有加密则先由解密单元 323 进行解密后才通过 USB 巨量储存层级控制器 310 送到 USB 操作系统 100 中。

请再配合图 2 所示，为上述数据保护装置 320 中的写入保护单元 321 对数据储存媒体 200 进行数据写入保护的動作流程，包括步骤 500~550，其中：

(500)：USB 操作系统传送 USB 巨量储存协议命令。

(510)：USB 协议命令处理。由 USB 巨量储存层级控制器 310 进行对 USB 操作系统 100 所送来命令进行判断处理。

(520)：判断是否为数据写入命令？如是则进行步骤(530)：如不是则进行步骤(520A)。

(520A)：执行其它命令程序。

(530)：使用者是否设定数据写入保护？如是则进行步骤(540)；如不是则进行步骤(530A)。

(530A)：将 USB 操作系统送来的数据写入数据储存媒体。

(540)：禁止数据写入数据储存媒体。

(550)：将禁止写入结果传回 USB 操作系统。

由以上步骤 500~550 所示的流程，可以显现写入保护单元 321 执行数据写入保护的動作过程，其意义是在说明该写入保护单元 321 可以由一原始的 USB 操作系统 100 设定成不可写入的保护，在该 USB 储存媒体读写器 400 插拉连结至另一 USB 操作系统 100 时，可以禁止该 USB 作业系统对数据储存媒体 200 进行数据写入，达到数据储存媒体 200 的数据保护功效。

请再参阅图 3 所示，是上述数据保护装置 320 中的加密单元 322 进行数据加密的处理流程，包括步骤 600~640，其中：

(600)：USB 操作系统传送 USB 巨量储存协议命令。

(610)：USB 协议命令处理。即由该由 USB 巨量储存层级控制器 310 进行对 USB 操作系统 100 所送来命令进行判断处理，并将该命令送到数据保护装置 320。

(620)：判断是否为数据写入命令？如是则进行步骤(630)：如不是则进

行步骤(620A)。

(620A): 执行其它命令程序。

(630): 使用者是否启用加密功能或原先数据储存媒体已被设定加密? 如是则进行步骤(640)); 如不是则进行步骤(630A)。

(630A): 将 USB 操作系统送来的数据直接写入数据储存媒体。

(640): 对数据加密后再写入数据储存媒体。即由加密单元 322 对 USB 操作系统 100 所送来要写入数据储存媒体 200 的数据进行加密后写入数据储存媒体 200 内。

以上各步骤显示加密单元 322 可以依使用者经 USB 操作系统下达数据储存媒体 200 写入数据加密或不加密设定, 来达到数据分级保密的功效。

请再配合图 4 所示, 为上述数据保护装置 320 中的解密单元 323 的解密执行流程, 包括步骤 700~740, 其中:

(700): USB 操作系统传送 USB 巨量储存协议命令。

(710): USB 协议命令处理。即由 USB 巨量储存层级控制器 310 进行对 USB 操作系统 100 所送来命令进行判断处理, 并将该命令送到数据保护装置 320。

(720): 判断是否为数据读取命令? 如是则进行步骤(730); 如不是则进行步骤(720A)。

(720A): 执行其它命令程序。

(730): 数据储存媒体是否被设定加密? 如是则进行步骤(740); 如不是则进行步骤(730A)。

(730): 直接将数据储存媒体的数据读入 USB 操作系统。

(740): 对数据自动解密后再读入 USB 操作系统。即由解密单元 323 对数据储存媒体 200 中所欲读取的数据进行解密, 再读入 USB 操作系统 100。

可由上述的各步骤了解本实用新型中对于已被加密设定的数据储存媒体 200 进行自动的数据解密再读入 USB 操作系统 100 中供使用的功能。

请再配合图 5 所示, 为本实用新型的数据安全装置 300 于实际应用上的较佳实施例, 其中, 该数据安全装置 300 装设在一 USB 储存媒体读写器 400 中, 该 USB 储存媒体读写器 400 在图 5 中所列的实施例为一 USB 读卡器型态,



可以对所连结的计算机主机 800，通过 USB 接口，以计算机主机 800 为设定操作的平台，对 USB 储存媒体读写器 400 所连结进行数据读、写的数据储存媒体 200，作相关的数据写入保护、加密及数据读出解密的操作，可以使数据储存媒体 200 内储存的数据不会被任意篡改、删除或窃取复制，达到本实用新型确保数据储存媒体内数据安全的目的。

本实用新型的创作精神，是在于以最为简捷有效的结构，来使如 CF、MMC、SM 及 SD 等存储器数据读、写，可由使用者依读、写需求分别设定写入保护、加密及解密功能，使数据储存媒体可以在不改变硬件线路的情况下，具有数据写入保护、加密及数据读出解密等功效。

以上图 1～图 5 所示本实用新型的 USB 储存媒体读写器的数据安全装置，其中所揭示的实施例说明及附图是为便于阐明本实用新型的技术内容及技术手段，而并非用作为对本实用新型的限定，只要在本实用新型的实质精神范围内，对以上所述实施例的变化、变型都将落在本实用新型权利要求书的范围内。

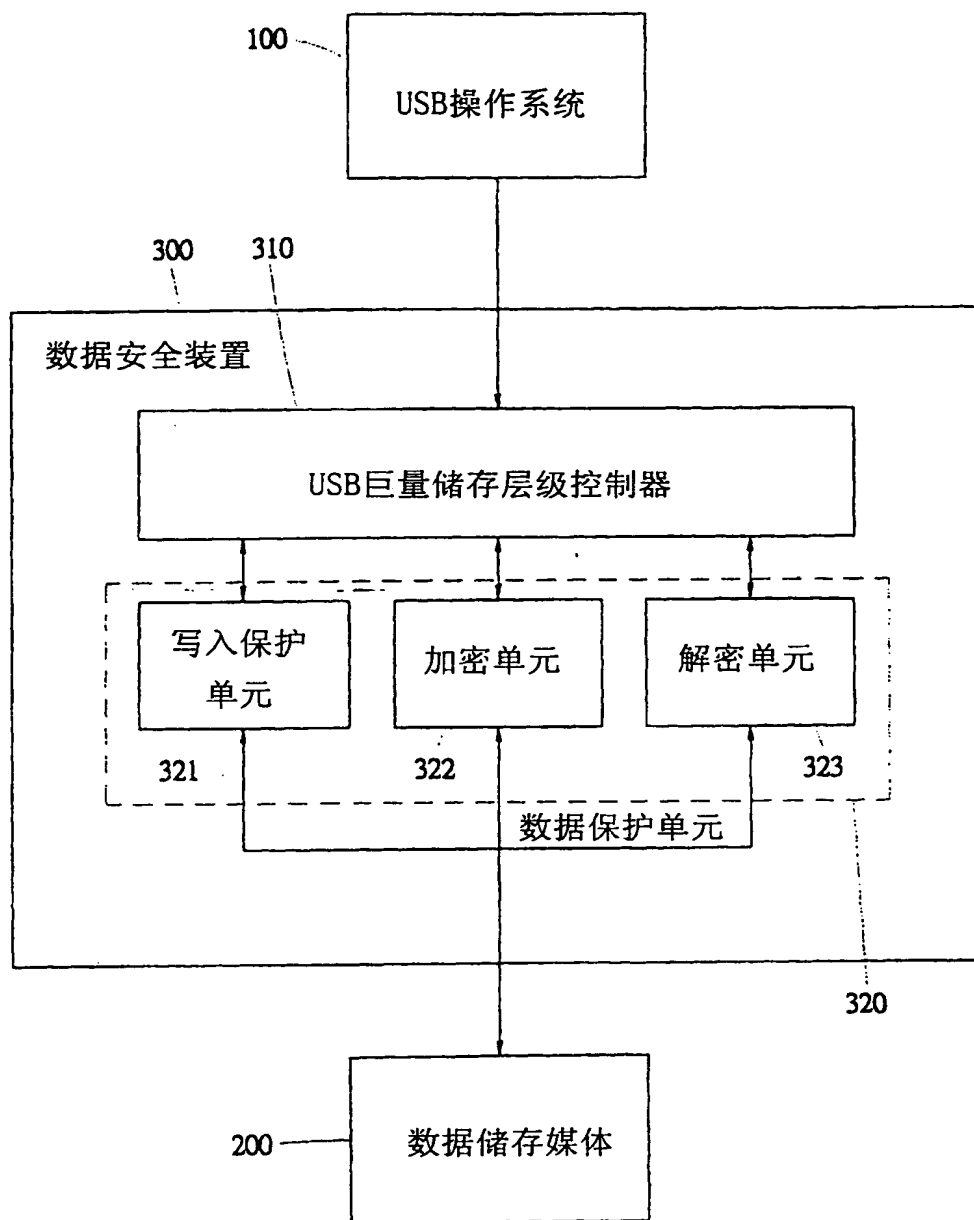


图 1

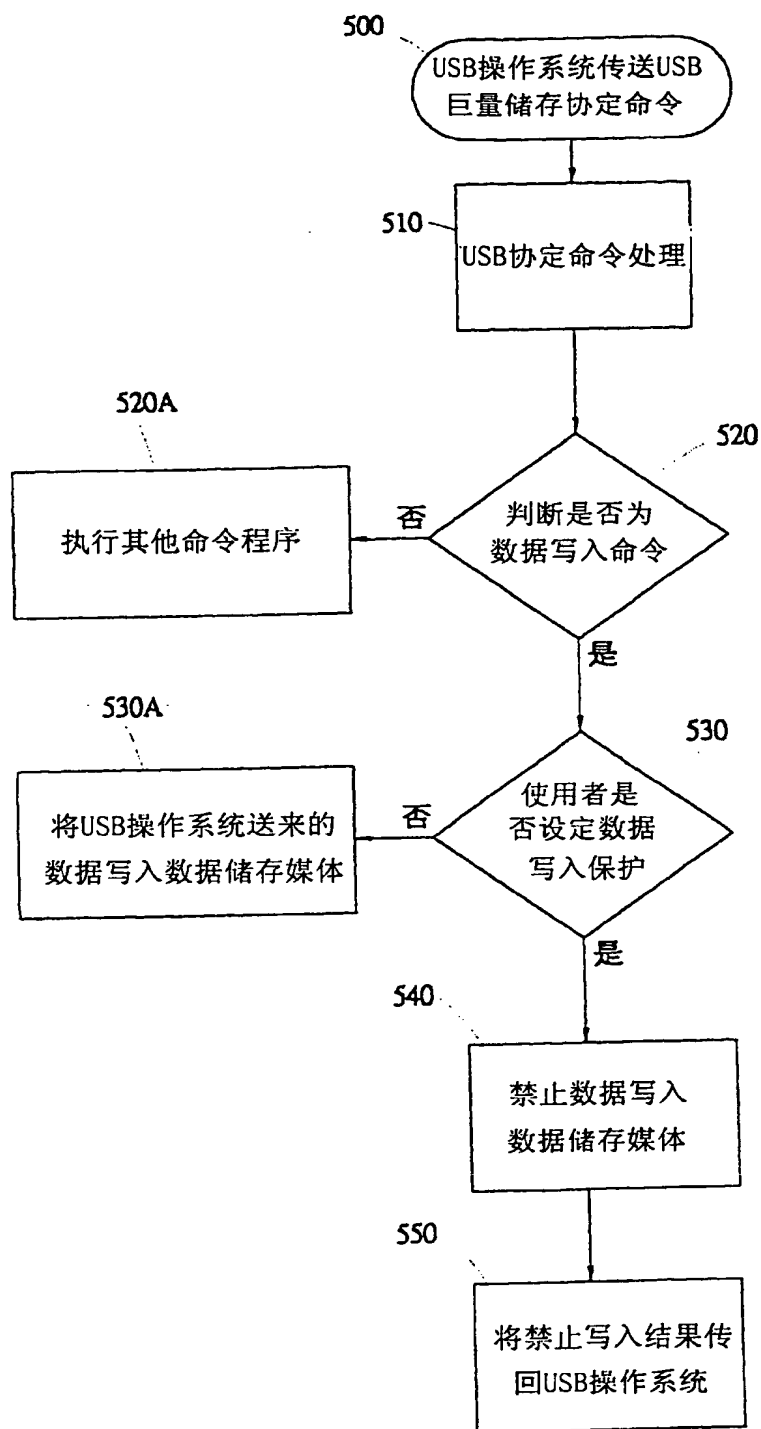


图 2

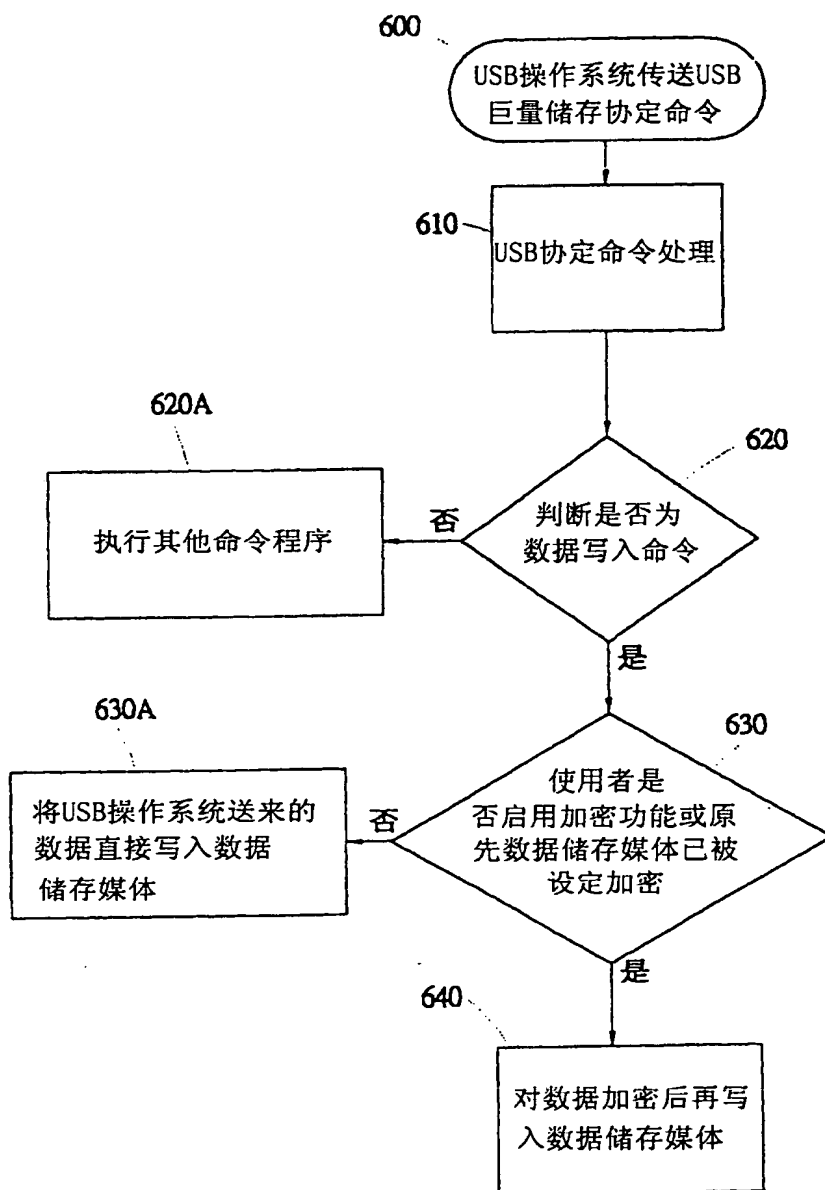


图 3

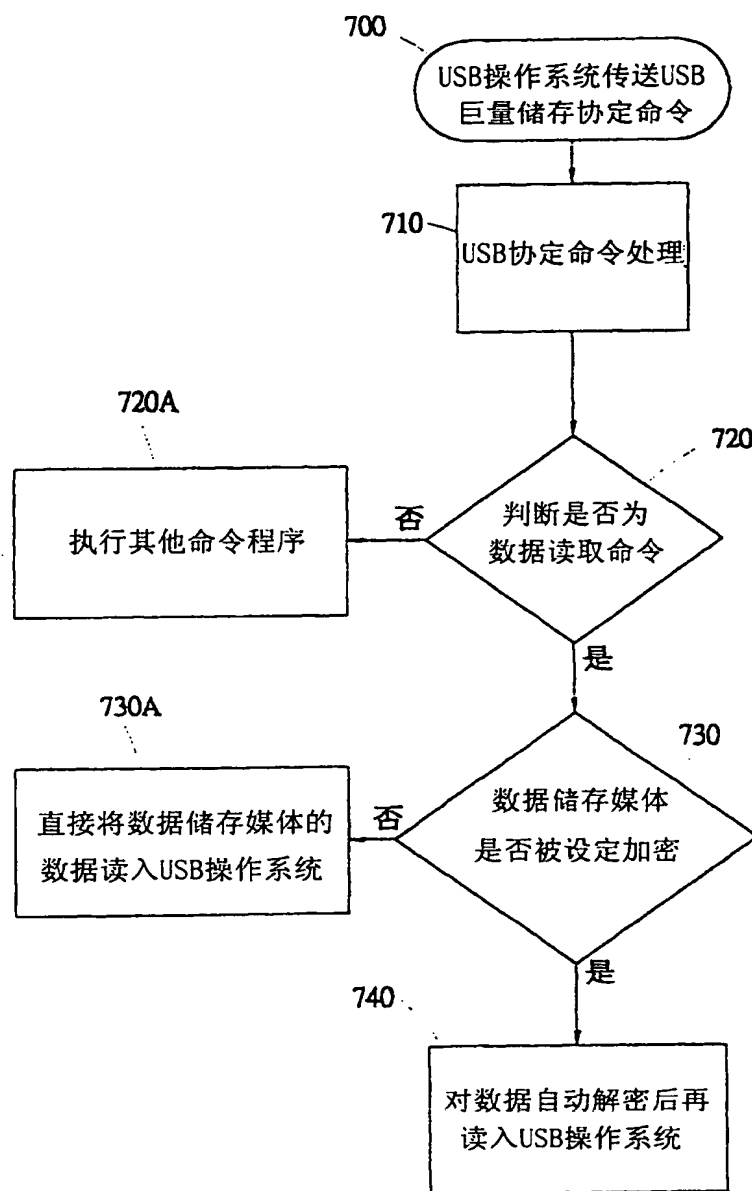


图 4

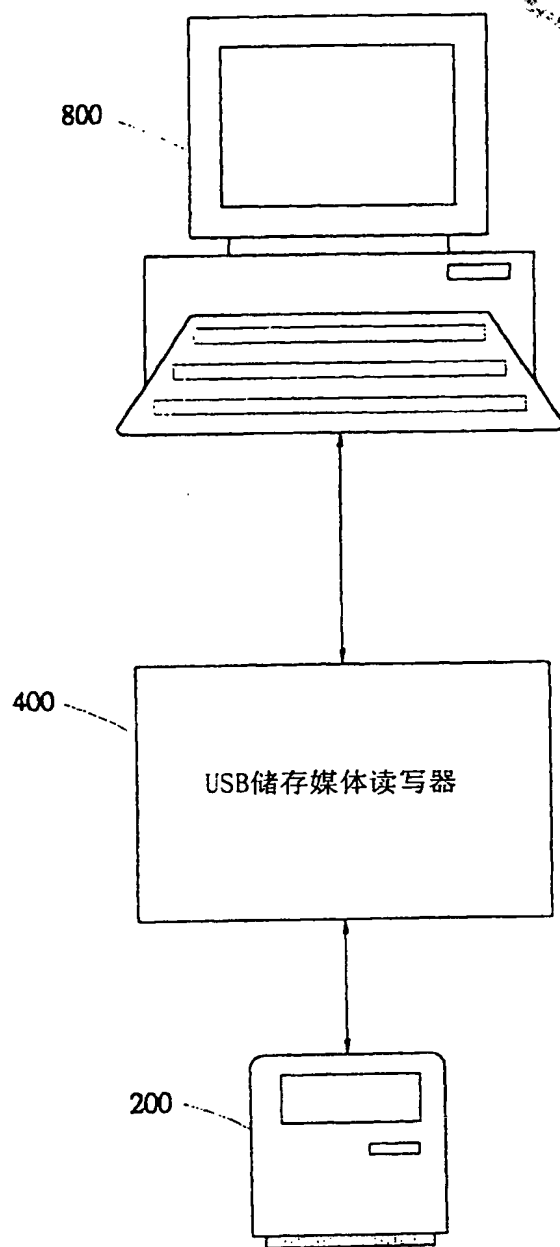


图 5